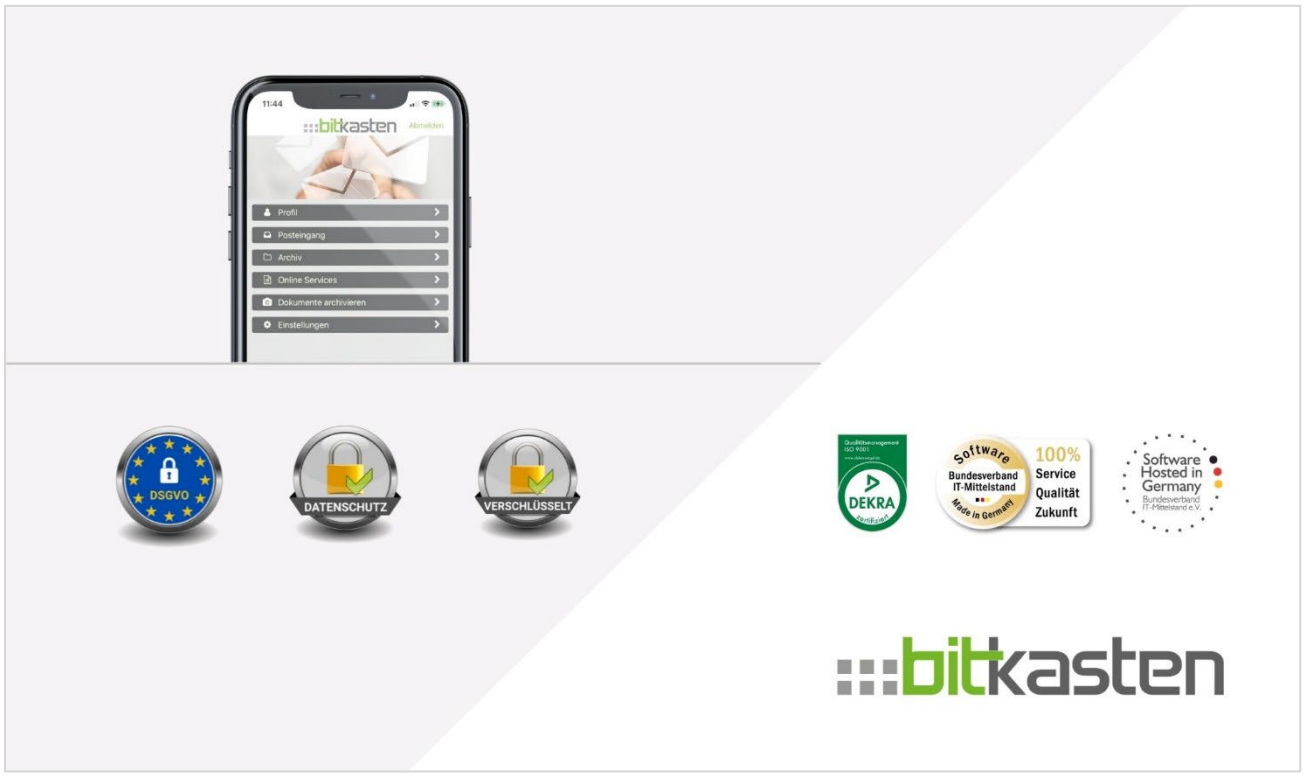
Rechtliche Risiken der Verwendung von E-Mail in der Kommunikation



Datum: 13. September 2022

Kontakt: Christian Gericke
christian@bitkasten.de

Inhaltsverzeichnis

Überblick bitkasten

Die bitkasten AG ist ein deutscher Software-as-a-Service (SaaS) und Clean-Tech-Anbieter für die vollständige Digitalisierung der Briefkommunikation und des Informationsaustauschs. Die Lösung ist der bitkasten, eine Digitalisierungs- und Kommunikationsplattform – ökologisch, nachhaltig und smart.

Mit dem bitkasten überbrücken Unternehmen die „letzte Meile" zu Kund:innen und Mitarbeitenden durch die Digitalisierung der Input- und Output-Prozesse. Dies erfolgt ohne aufwändiges IT-Projekt innerhalb kurzer Zeit durch Verwendung bestehender Druckdaten und bekannte Postadressen. Die nachhaltige Briefkommunikation, digital und ohne Druck & Transport, führt zu einer Halbierung der Druck-, Porto- und Prozesskosten mit einem ROI innerhalb von wenigen Wochen.

Briefe werden rechtssicher an den digitalen, smarten Briefkasten zugestellt. Der bitkasten steht für schnelle Kommunikation wie E-Mail, aber ohne E-Mail-Adresse, dafür sicher und DSGVO-konform. Die Identifizierung und digitale Zustellung der Kommunikation erfolgen mittels der bekannten Postadresse über den elektronischen Personalausweis oder Kennung.

Für Empfänger:innen funktioniert die Kommunikation im bitkasten ohne Medienbruch via App oder Web. Der bitkasten empfängt Post digital von allen teilnehmenden Versendern, stellt die Möglichkeit einer digitalen Signatur bereit und übermittelt Daten an ERP,- CRM-, HR-Systeme oder direkt an Fachverfahren im kommunalen Umfeld. Durch Abbildung von Prozessen, Eingabemöglichkeiten oder Formularen im geschlossenen System des bitkasten, ist der/die Empfänger:in sicher mit dem Unternehmen verbunden.

Aufgabe

Gefragt ist nach einer Kurzstellungnahme zu Risiken der Verwendung von E-Mail aus rechtlicher Sicht.

Auftraggeber der vorliegenden Stellungnahme ist die bitkasten AG, Wallensteinstraße 63, 90431 Nürnberg. Ersteller ist die Kanzlei SNP Schlawien Partnerschaft mbB, München.

Rechtliches Kurzgutachten

1 Kleingedrucktes

Die aufgeführten Urteile, Tipps und Beiträge sind nach bestem Wissen und Gewissen sorgfältig zusammengestellt. Es wird kein Anspruch auf Vollständigkeit und Ausschließlichkeit der Inhalte gestellt. Die zur Verfügung gestellten Informationen ersetzen keine individuelle juristische Beratung. Sie sind daher unverbindlich. Es wird keine Gewähr dafür übernommen, dass im Streitfall den hier dargelegten Urteilen und Ansichten gefolgt wird. Eine Haftung für die veröffentlichten Inhalte wird daher nicht übernommen.

2 Übersicht

E-Mail ist neben Messenger-Diensten das verbreitetste elektronische Kommunikationsmittel. Wurden im Jahr 2000 noch 32,3 Milliarden E-Mails in Deutschland versendet (ohne Spam), waren es im Jahr 2018 848,1 Milliarden, in der Tendenz weiter steigend.[1] Vorhersagen, dass die E-Mail durch neue Kommunikationsformen wie Messenger und Collaboration-Tools an Bedeutung verlieren wird, bestätigen sich nicht.[2]

Diese weite Verbreitung bringt es mit sich, dass E-Mail vielfältig im geschäftlichen und rechtlichen Verkehr zur Abgabe von Willenserklärungen und zum Vertragsschluss eingesetzt wird. Sie dient zudem jeder Art von Kommunikation und der Übermittlung von Dokumenten, auch in sensiblen Bereichen. Ihr Einsatz wirft dabei eine Reihe von Fragen auf:

- Die Rolle von E-Mail im Rechtsverkehr, insbesondere bei der Abgabe von Willenserklärungen und Vertragsschluss; hier insbesondere die Authentizität und Integrität von E-Mail;
- damit verbunden Fragen des Zugangs von Willenserklärungen beim Empfänger und des
- Beweiswerts von E-Mail im Fall von Streitigkeiten;

[1] Laut Statista.de, abrufbar unter https://de.statista.com/statistik/daten/studie/392576/umfrage/anzahl-der-versendeten-e-mails-in-deutschland-pro-jahr.

[2] Vgl. Reddox-Studie „E-Mail 2020 – Status der E-Mail in Deutschland", in Zusammenfassung und als Text abrufbar unter https://www.reddoxx.com/studie-email-2020/.

- Fragen der Vertraulichkeit und des Datenschutzes bei der Verwendung von E-Mail, sowie
- E-Mail als Gefahrenquelle und Angriffsvektor (Spam, DDoS, Schadsoftware).

Unter all diesen Aspekten weist E-Mail Defizite auf. Diese lassen sich durch vielfältige Maßnahmen mindern oder sogar beseitigen. Solche Maßnahmen sind allerdings mit teils erheblichem Aufwand verbunden, müssten in einigen Fällen mit dem Empfänger von E-Mails abgestimmt werden, und werden in der Praxis daher oft nicht oder nur zögerlich ein- und umgesetzt. Im täglichen Einsatz weist E-Mail daher aus rechtlicher Sicht erhebliche Defizite auf.

3 Technische Funktionsweise von E-Mail

Da sich der Hintergrund einer Reihe der genannten Fragen aus der technischen Funktionsweise von E-Mail erklärt, sei diese kurz dargestellt.

3.1 Empfangs- und Sendesystem

Ein E-Mail-System besteht nutzerseitig aus:

- einem Posteingangsserver, der permanent Nachrichten entgegennimmt und diese in "Postfächern" für die Nutzer bereitlegt (POP3- oder IMAP-Server),
- einem Postausgangsserver, an den gesendete E-Mail-Nachrichten übergeben werden und der diese an das weltweite E-Mail-Verteilungssystem weiterleitet (SMTP-Server), sowie
- einem E-Mail-Client.

Der E-Mail-Client ist ein Programm, das entweder auf dem Gerät des Teilnehmers installiert sein kann oder (etwa MS-Outlook) oder über eine Internetseite zur Verfügung steht.[3]

3.2 Transport, Übertragung, Server

Die E-Mail wird (in der Regel) nicht selbst durch den Sender zugestellt, sondern von diesem an einen Mailserver übergeben, der sich um den Weitertransport kümmert. Der Transport ist dabei eine gewöhnliche TCP/IP-Kommunikation unter Verwendung des Protokolls SMTP (Simple Mail Transfer Protocol). Beim Transport einer E-Mail durch das Internet können dabei unterschiedlich viele Rechner beteiligt sein. Der Transportweg lässt sich durch den jeweiligen Eintrag der beteiligten Server in den Header (der Felder wie From, To, CC, Subject, Date, und andere Metainformationen enthält) der transportierten E-Mail nachvollziehen. Allerdings muss nicht jeder dieser Einträge vertrauenswürdig sein (dazu siehe unten).[4]

---

[3] Universität Bamberg, Funktionsweise von E-Mail-Systemen, abgerufen unter https://www.uni-bamberg.de/its/dienstleistungen/mail/weitere-informationen-zu-e-mail/funktionsweise-von-e-mail-systemen.

[4] Zu diesen Punkten ausführlich und mit technischen Erläuterungen: Rehbein, Transport von E-Mails - RFC 2821, abrufbar unter http://www.daniel-rehbein.de/rfc2821.html.

3.2.1 Unverschlüsselte E-Mail

Das SMTP-Protokoll transportiert E-Mails standardmäßig unverschlüsselt im Klartext. E-Mails sind daher anfällig für die Offenlegung von Informationen. Unbefugte können die übermittelten Informationen zur Kenntnis nehmen und manipulieren, ohne dass Absender und Empfänger der E-Mail dies bemerken. Eine unverschlüsselte E-Mail ist also offener als eine mit Bleistift geschriebene Postkarte.[5]

Heute verwenden die meisten Provider allerdings eine Transportverschlüsselung. Jedoch hängt die Verfügbarkeit einer Verschlüsselung eben von den E-Mail-Providern ab. Dies bedeutet, dass E-Mails bei bestimmten E-Mail-Providern unverschlüsselt über das Internet gesendet werden.

3.2.2 Transportverschlüsselung

Die Transportverschlüsselung ist eine Punkt-zu-Punkt-Verschlüsselung. Hierbei wird zwischen den beteiligten Geräten (des Absenders und dessen E-Mail-Provider, den beteiligten Servern etc.) eine Verbindung aufgebaut und diese z.B. gemäß dem weit verbreiteten Protokoll "Transport Layer Security" (TLS, dem Nachfolger des SSL-Protokolls) verschlüsselt, das eigenständig auf SMPT aufsetzt. Unter der Annahme, dass die beteiligten Geräte sowohl auf der Absender- als auch auf der Empfängerseite eine verschlüsselte Kommunikation unterstützen, kann ein Angreifer, der die Kommunikation zwischen den E-Mail-Servern ausspäht, keinen Sniffer verwenden, um den Inhalt der E-Mail einzusehen.[6]

Alle Daten, die zwischen beiden Kommunikationspartnern ausgetauscht werden, sind dann während des Versands verschlüsselt. Die E-Mail wird beim Versand über unterschiedliche Knotenpunkte im Web zum Empfänger weitergeleitet und ist an diesen Punkten und dazwischen nicht unbedingt verschlüsselt. Sowohl beim E-Mail-Anbieter als auch an den Knotenpunkten des Versands liegt die E-Mail dann im Klartext vor.[7] Auch Internet-Kriminelle könnten einen "Man-in-the-Middle-Angriff" starten, der auf diese Punkte ausgerichtet ist. Ist ein solcher Angriff erfolgreich, kann die E-Mail abgefangen, kopiert oder verändert werden.[8]

Salopp gesagt lässt sich die Transportverschlüsselung einer E-Mail mit dem Transport einer Postkarte in einem verschlossenen Transportbehälter zwischen Postverteilzentren und Empfänger vergleichen.[9]

Aus Sicht des Verwenders einer E-Mail genügt es zur Sicherstellung der Transportversicherung nicht, diese selbst zu beherrschen. Denn ohne weiteres kann sich der Absender nicht sicher sein, dass der Empfänger (oder in der Transportkette beteiligte Server) die verwendete Transportverschlüsselung unterstützen. Dies

---

[5] Mit diesem Bild: Landesbeauftragter für den Datenschutz Sachsen-Anhalt im Landesportal, https://datenschutz.sachsen-anhalt.de/landesbeauftragter/kontakt/wichtige-hinweise-zum-e-mail-versand/, der auf unverschlüsselte E-Mails auch nur per Briefpost antwortet.

[6] Vgl. Wikipedia-Eintrag Email Encryption abrufbar unter https://en.wikipedia.org/wiki/Email_encryption.

[7] Für TLS: Wikipedia-Eintrag zu Transport Layer Security, abrufbar unter https://de.wikipedia.org/wiki/Transport_Layer_Security#Vor-_und_Nachteile.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI), E-Mail Verschlüsselung, abrufbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/e-mail-verschluesselung_node.html.

[9] Tätigkeitsbericht 2019 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, S. 131.

kann sicher nur umgesetzt werden, indem der Sender sicherstellt, dass ohne Vorhandensein einer sicheren Verbindungsmöglichkeit die E-Mail-Übertragung nicht vorgenommen wird.[10]

In der Praxis heißt das, dass ggf. E-Mails nicht versandt werden können.

3.2.3 Ende-zu-Ende-Verschlüsselung

Im Unterschied zur Transportverschlüsselung werden bei der Ende-zu-Ende-Verschlüsselung nicht die einzelnen Abschnitte im Versandkanal verschlüsselt, sondern jede einzelne E-Mail selbst. Nur Sender und Empfänger können die E-Mail im Klartext lesen, wenn diese über den notwendigen Schlüssel verfügen. Weder die beteiligten E-Mail-Anbieter können die E-Mail lesen, noch haben potenzielle Angreifer die Möglichkeit, die E-Mails unterwegs zu manipulieren. Damit erfüllt nur diese Technik die drei Ziele der Verschlüsselung im Internet: Vertraulichkeit, Authentizität, Integrität.[11]

Der Einsatz einer solchen Verschlüsselung ist jedoch vergleichsweise komplex. Der Anwender muss bei der Ende-zu-Ende-Verschlüsselung selbst aktiv werden, um die Technologie nutzen zu können, jedenfalls, wenn diese von Client zu Client erfolgen soll (also bereits auf dem Erst- und Letztserver verschlüsselte E-Mails vorliegen sollen). In der Praxis werden in Unternehmen oder Organisationen daher ggf. E-Mails auf dem Mailserver / Gateway des Unternehmens verschlüsselt, liegen bis dahin also unverschlüsselt vor.[12]

4 Rechtliche Aspekte

E-Mail wird vielfältig im Rechtsverkehr eingesetzt. Dies betrifft die Abgabe von Willenserklärungen und Vertragsschlüsse, aber auch die Kommunikation im geschäftlichen Bereich allgemein. Es stellt sich daher die Frage, ob E-Mail für diese Zwecke geeignet ist, ob spezifische Gefahren bestehen, und wie hoch der Beweiswert von E-Mails im Rahmen eines möglichen Streits ist.

4.1 E-Mail im Rechtsverkehr, Abgabe von Willenserklärungen

Aus rechtlicher Sicht handelt es sich bei jeder E-Mail um ein elektronisches Dokument.[13] Die Rechtsordnung regelt teils, wie etwa Aspekte wie Beweiskraft im Prozess oder Wahrung von Formvorschriften im Zivilrecht zu bewerten sind. Es erkennt dabei an, dass die reinen Datenpakete einer E-Mail anfällig für Manipulationen oder auch Störungen in Versand und Zustellung sind.[14] Denn ohne weiteres lässt sich bei

[10] So gefordert in BSI-Richtlinie TR-03108-1, Secure E-Mail Transport, Vers. 1.0.2, 17.2.2022, dort 2.1.2.1: „If a secure connection cannot be created, although cryptographic information is present, the e-mail MUST NOT be sent."

[11] BSI, E-Mail-Verschlüsselung, a.a.O.

[12] Vgl. zur Problematik Wikipedia-Eintrag E-Mail-Verschlüsselung, a.a.O.

[13] Vgl. Einsele, Münchener Kommentar zum BGB, 9. Auflage 2021, § 126a Rn. 3.

[14] Vgl. hier Al-Deb'i, Weidt: Die E-Mail im Zivilprozess, JA 2017, 618.

einer E-Mail nicht feststellen, wer sie versendet hat und ob der Inhalt der E-Mail unverändert beim Empfänger eingegangen ist.

Betroffen sind hier die Gesichtspunkte der Authentizität und Integrität. Dabei ist mit der Authentizität einer E-Mail gemeint, dass sichergestellt ist, dass die E-Mail auch wirklich vom Absender stammt, also ein Original ist und keine betrügerische Fälschung. Als Integrität bezeichnet man das Schutzziel, dass der E-Mail-Inhalt bei der Übertragung vollständig und unverändert bleibt.[15] Komplexe rechtliche Fragen wirft zudem der Zugang von Willenserklärungen per E-Mail auf.

4.1.1 Authentizität

Damit wirksam und nachweisbar eine Willenserklärung per E-Mail abgegeben oder sonst rechtlich relevante Erklärungen gemacht werden können, muss zunächst klar sein, wer die entsprechende E-Mail übersandt hat. Dies betrifft die Frage der Authentizität.

Absenderadressen von E-Mails können mit geringem Aufwand beliebig gefälscht werden (sog. Spoofing).[16] Hinter dem in einer E-Mail angezeigten Namen einer Person oder Organisation kann sich ein ganz anderer Absender verbergen. Dies ist teils aus technischen und organisatorischen Gründen gerade bei Unternehmen beabsichtigt.[17] Sehr häufig aber ist dies bei illegalen Aktivitäten der Fall, wie Spam-Versand oder dem Versuch, den Computer eines Nutzers mit Schadsoftware zu infizieren.[18]

Die Echtheit des Absenders lässt sich teils durch die Verifikation des E-Mail-Headers ermitteln. Der Header kann im E-Mail-Programm oder auch in einem Texteditor angezeigt werden. In den mit "Received From" bezeichneten Zeilen können Nutzer den Weg der Mail verfolgen, der Versender findet sich in der letzten Received From-Zeile. Teilweise manipulieren Angreifer aber auch die Received-Zeilen, sodass es schwieriger wird, die tatsächliche Herkunft der E-Mail festzustellen.[19]

Ohne weitere Maßnahmen lässt sich daher die Authentizität einer E-Mail nicht feststellen (vgl. unten 4.1.4.1 - Beweiswert).

4.1.2 Integrität

Selbst wenn feststeht, dass eine Willenserklärung abgegeben oder eine in anderer Weise relevante E-Mail übermittelt wurde und von wem, ist im Fall der Verwendung von E-Mail nicht ohne weiteres sicher nach-

---

[15] Schmidt/Pruß in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 3 Technische Grundlagen des Internets, Rn 184.

[16] Vgl. Deusch/Eggendorfer in Taeger/Pohle, Computerrechts-Handbuch, Werkstand: 36. EL Februar 2021, 50.1 IT-Sicherheit Rn. 40.

[17] Vgl. Wikipedia-Eintrag „Mail-Spoofing", abrufbar unter https://de.wikipedia.org/wiki/Mail-Spoofing.

[18] Vgl. mit Diskussion verschiedener Konstellationen Drozhzhin, Deshalb können E-Mails gefälscht werden, 10 Feb 2020, abrufbar unter https://www.kaspersky.de/blog/36c3-fake-emails/21957/.

[19] Bundesamt für Sicherheit in der Informationstechnik, Sicherheits-Irrtümer: E-Mail-Sicherheit; abrufbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Sicherheitsirrtuemer/irrtuemer-e-mail-sicherheit.html?nn=131822.

zuweisen, dass der Inhalt der E-Mail authentisch ist oder verändert wurde. Dies betrifft mithin den Gesichtspunkt der Integrität.

Fallgestaltungen beginnen hier schon beim „einfachen" Verändern einer empfangenen E-Mail im E-Mail-Client selbst in der Weiterleitung, um etwa vorzutäuschen, der ursprüngliche Sender habe eine bestimmte Erklärung abgeben oder Aussage getätigt.[20]

4.1.3 Zugang

Werden Willenserklärungen über E-Mail abgegeben, so hängt deren Wirksamkeit in der Regel vom Zugang beim Empfänger ab, § 130 Abs. 1 S. 1 BGB. Die damit spezifisch im Fall von E-Mail verbundenen Fragestellungen sind vielfältig und komplex.[21]

Nach der sog. Empfangstheorie ist eine Willenserklärung im Sinne von § 130 Abs. 1 S. 1 BGB zugegangen, wenn die Erklärung in den Machtbereich des Empfängers gelangt ist, sodass dieser die Möglichkeit der Kenntnisnahme hat und mit dieser unter normalen Umständen zu rechnen ist.[22] Dies ist der Fall, wenn eine E-Mail abrufbar in der Mailbox des Empfängers abgespeichert ist.[23]

Wann dies der Fall ist, ist für den Absender oft nicht zu ermitteln oder gar nachzuweisen. Denn E-Mail kennt Standards für Empfangsbestätigungen (Delivery Status Notification, Message Disposition Notification).[24] Einige E-Mail-Server bzw. Clients (etwa MS Outlook) ermöglichen es, solche Bestätigungen anzufordern. Dies wird aber nicht notwendigerweise vom Client des Empfängers unterstützt und ist zudem in der Regel kein automatisierter Vorgang, sondern bedarf der Einrichtung oder Bestätigung durch den Nutzer.[25] Ein rechtssicherer Nachweis über den Zeitpunkt des Zugangs ist damit oft nicht zu erlangen. Insbesondere begründet der Beweis des Absendens einer E-Mail auch keinen Anscheinsbeweis für deren Zugang.[26] Ebenso gilt dies dann, wenn der Absender einen Dritten oder sich selbst in Kopie setzt: es handelt sich hier um technisch verschiedene Übermittlungsvorgänge.[27]

Hinzu kommt, dass das Transportrisiko (Verlust- und Verzögerungsrisiko) beim Erklärenden liegt.[28] Denn dieser hat gerade das Transportmittel E-Mail mit all seinen Schwächen gewählt.[29] Dafür spricht der

---

[20] Etwa im Urteil des Schweizer Bundesgerichtes vom 22. Oktober 2012, 6B_130/2012.

[21] Vgl. im Überblick Beh, Aktuelle Probleme beim Zugang von E-Mails, ZJS 3/2019 S. 165 ff.

[22] Spindler, Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 130 BGB Rn. 2.

[23] LAG Berlin-Brandenburg BeckRS 2013, 66632.

[24] Vgl. zu Technik und Standards die entsprechenden Einträge bei Wikipedia: https://de.wikipedia.org/wiki/Message_Disposition_Notification, https://de.wikipedia.org/wiki/Delivery_Status_Notification.

[25] Wie vor.

[26] Ortner Handbuch Multimedia-Recht, Werkstand: 58. EL März 2022, Teil 13.2 Beweisqualität elektronischer Dokumente, Rn. 47.

[27] Willems: Beweis und Beweislastverteilung bei Zugang einer E-Mail - Fallkonstellationen unter besonderer Betrachtung elektronischer Bewerbungen, MMR 2013, 551, 553.

[28] BGH NJW 1995, 665, 667.

[29] Ann, in Leipold (Hrsg.), Rechtsfragen des Internet und der Informationsgesellschaft, 2002, S. 175 (179); Ultsch, NJW 1997, 3007 (3008); Weiler, JuS 2005, 788 (789).

Rechtsgedanke des § 120 BGB, der das Fehlerrisiko und damit den Transport dem Erklärenden zurechnet.[30]

Auch wenn eine E-Mail dem Empfänger zugegangen ist, heißt dies nach überwiegend vertretener Ansicht nicht, dass ggf. als Anhang übermittelte Dokumente ebenfalls zugegangen sind. Vielmehr ist dies für den Anhang erst dann gegeben, wenn dieser vom Empfänger auch tatsächlich zur Kenntnis genommen wird.[31] Dies wird damit begründet, dass der Versender einer E-Mail damit rechnen muss, dass der Empfänger einer E-Mail mit Anhang eben diesen Anhang wegen der erhöhten Gefahr der Übertragung von Schadsoftware und Viren nicht öffnet.[32] Im Ergebnis bestehen hinsichtlich des Zugangs elektronischer Willenserklärungen in E-Mail-Anhängen bereits auf materieller Ebene so schwere Unsicherheiten, dass rechtssichere rechtsgeschäftliche Kommunikation mittels dieser faktisch nicht für möglich gehalten wird.[33]

Weitere Probleme treten auf, wenn die Mailbox des Empfängers überfüllt ist, Mails durch Spam-Filter blockiert oder gar vom Provider direkt – und oft ohne weitere Mitteilung an Absender oder Empfänger – gelöscht werden.

4.1.4 Rechtliche Konsequenzen

Aus diesen Gründen findet die Rechtsordnung für E-Mail eine differenzierte Bewertung betreffend Form und Beweiswert.

4.1.4.1 Beweiswert[34]

E-Mails haben wenig Beweiskraft, da der Sender bei den herkömmlichen Protokollen und Log-Mechanismen nicht längerfristig die Möglichkeit hat, zu beweisen, wann er was an wen versendet, ob der Empfänger die E-Mail erhalten hat oder ob sie tatsächlich abgesendet wurde (siehe dazu die Diskussion oben).[35] Eine einfache E-Mail ist dabei Gegenstand des Augenscheinbeweises, der durch Vorlegung oder Übermittlung der Datei angetreten wird, § 371 Abs. 1 S. 2 ZPO. Ohne qualifizierte elektronische Signatur bleibt es bei der freien Beweiswürdigung des Gerichts gemäß § 286 ZPO. Eine erhöhte Beweiskraft, z. B. durch analoge Anwendung der Beweisvorschriften des § 371 a ZPO, kann der E-Mail nicht zugebilligt werden.[36]

---

[30] BGH NJW 1995, 665 (667).

[31] Vgl. Bornkamm, Köhler/Bornkamm/Feddersen, Kommentar zum Gesetz gegen den unlauteren Wettbewerb, 34. Aufl. 2016, § 12 Rn. 1.35a.

[32] Greiner, Kalle, Ungeklärte Fragen des Wirksamwerdens empfangsbedürftiger Willenserklärungen – im Grundsatz und bei Verwendung digitaler Kommunikationswege, JZ 2018, 535, 539; differenzierend hier allerdings Gomille in Gsell/Krüger/Lorenz/Reymann, beck-online GROSSKOMMENTAR Stand: 01.04.2020, § 130 BGB Rn. 77.

[33] Vgl. nur Hengstberger, Zugang von Willenserklärungen in E-Mail-Anhängen, NJW 2022, 1780, 1783; Besprechung zu OLG Hamm, Beschluss vom 09.03.2022 - 4 W 119/20.

[34] Vgl. im Überblick mit zahlreichen Nachweisen bei Al-Deb'i/Weidtm, Die E-Mail im Zivilprozess, JA 2017, 618.

[35] Vgl. Schmidt/Pruß, Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, Rn 186.

[36] AG Bonn Urt. v. 25. 10. 2001 – 3 C 193/01, NJW-RR 2002, 1363, LG Frankenthal Urt. v. 9. 9. 2014 – 6 O 37/14, BeckRS 2016, 17920, Wagner JuS 2016, 29, 31.

Teils wird der Beweiswert von E-Mails allerdings differenzierter betrachtet. Der schlichte Hinweis auf die Manipulierbarkeit ist zur Verneinung des Beweiswertes zu pauschal. Vielmehr sollte das Gericht, das über den Beweiswert einer E-Mail zu urteilen hat, umfassend abwägen. In Betracht gezogen werden müsse etwa die technische Versiertheit der beweisführenden Partei.[37]

Dem ist nur zum Teil zuzustimmen, denn hier wird die Komplexität der Manipulation einer E-Mail überschätzt. Dies ist in der Praxis einfach. Zu Recht wird darauf hingewiesen, dass dies jeder weiß, der bereits einmal Spam-Nachrichten von einer vermeintlich bekannten E-Mail-Adresse erhalten hat.[38]

4.1.4.2 Form

Auch hinsichtlich der Form trägt das Zivilrecht den vorstehend diskutierten Umständen Rechnung. Die einfache E-Mail wahrt die Textform, § 126 b BGB.[39] Durch eine solche E-Mail können somit Willenserklärungen abgegeben und Verträge geschlossen werden, soweit keine strengere Form (insbesondere Schriftform) vorgeschrieben ist.

Fragen der Authentizität, Integrität und des Zugangs bleiben davon aber unberührt (siehe oben).

4.1.4.3 Lösungsmöglichkeiten und damit verbundene Aufwände

Sowohl ggf. erforderliche Schriftform als auch das Bedürfnis nach Authentizität[40] und Integrität[41] kann durch die Verwendung von E-Mail-Signaturen befriedigt werden. In Betracht kommt insbesondere die qualifizierte elektronische Signatur, die in § 126 a Abs. 1 BGB geregelt ist.

Die Verwendung der elektronischen Form bedarf jedoch eines erheblichen technischen und intellektuellen Aufwands. Der Anwender (Aussteller des elektronischen Dokuments) benötigt: geeignete Hard- und Software, ein qualifiziertes Zertifikat von einem qualifizierten Vertrauensdiensteanbieter i.S.d. eIDASVO, das bestimmte Angaben enthalten und eine qualifizierte elektronische Signatur tragen muss.[42] Viele Vertrauensdiensteanbieter, hier insbesondere Plattformbetreiber, bemühen sich, den Prozess der Bereitstellung dieser Voraussetzungen anwenderfreundlich zu steuern. Dennoch bleibt der Unterzeichnungsprozess oft (noch) ungewohnt und sperrig.[43]

4.1.4.4 Zwischenfazit

Die Sicherstellung in Integrität und Authentizität der E-Mail ist durch Verwendung qualifizierter elektronischer Signaturen möglich. Der Aufwand macht faktisch aus der an sich einfach zu bedienenden E-Mail

---

[37] Al-Deb'i/Weidtm, aaO.

[38] Ortner, Handbuch Multimedia-Recht, Werkstand: 57. EL September 2021, Teil 13.2 Beweisqualität elektronischer Dokumente, Rn. 46.

[39] Statt vieler: Einsele in Münchener Kommentar zum BGB, 9. Auflage 2021, § 126b BGB, Rn. 11.

[40] Vgl. hier Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999, Begründung Punkt (5).

[41] Computerwoche, E-Mail-Sicherheit: Das digitale Postgeheimnis wahren, 29.04.2009, abrufbar unter https://www.computerwoche.de/a/das-digitale-postgeheimnis-wahren,1894253,2.

[42] Mansel (der allerdings noch das SigG zitiert) in Jauernig, Bürgerliches Gesetzbuch, 18. Auflage 2021, § 126a Rn. 1.

[43] Selbst für umfangreiche Transaktionen: Meyer-Sparenberg in Meyer-Sparenberg/Jäckle, Beck'sches M&A-Handbuch, 2. Auflage 2022, § 51 Rn. 80.

ein Expertenwerkzeug.[44] Hinzu kommt, dass elektronische Signaturen allein die sich unter dem Gesichtspunkt der Vertraulichkeit stellenden Fragen nicht lösen, hierzu benötigt es Verschlüsselung (s. u.).[45] Auch Fragen des Zugangs werden durch elektronische Signaturen nicht berührt

4.2 Datenschutz und Vertraulichkeit

E-Mail-Adressen sind personenbezogene Daten. Ebenso die per E-Mail übertragenen Inhalte, sofern diese einen Personenbezug aufweisen, was in der Regel der Fall ist. Diese Daten unterliegen damit den datenschutzrechtlichen Vorschriften, insbesondere der DSGVO. Ihre Verarbeitung bedarf einer Rechtsgrundlage und die Vorgaben der Datenschutzgesetze sind einzuhalten. Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO, welche die Sicherheit der Datenverarbeitung betreffen, müssen sich auch auf die Verwendung von E-Mail beziehen.

Verantwortliche und Auftragsverarbeiter sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen.[46]

Kommen sie diesen Pflichten nicht nach, begründet dies einen Rechtsverstoß, der Maßnahmen der Aufsichtsbehörden und Bußgelder nach sich ziehen kann, aber auch zivilrechtliche Ansprüche auf Auskunft, Unterlassung, Sicherstellung der Betroffenenrechte nach der DSGVO und Schadensersatz begründen. In bestimmten Fällen, insbesondere bei Berufsgeheimnisträgern, kommen zudem strafrechtliche Verstöße in Betracht.

Zu beachten ist hier, dass datenschutzrechtliche Verstöße bereits dann vorliegen, wenn technisch-organisatorische Maßnahmen nicht im erforderlichen Maße getroffen werden, mithin eine Gefahr für personenbezogene Daten geschaffen wird. Dass diese tatsächlich abfließen oder kompromittiert werden, ist nicht erforderlich.

4.2.1 Erforderliche Maßnahmen für E-Mails mit gewöhnlichem Risiko

Bei der Verarbeitung personenbezogener Daten durch E-Mail sind ausreichende technisch-organisatorische Maßnahmen zu treffen, Art. 32 DSGVO.

4.2.1.1 Technische Maßnahmen, insbesondere Verschlüsselung

[44] Vgl. zur elektronischen Akte bei Gericht (JKomG) kritisch: Hähnchen, Elektronische Akten bei Gericht - Chancen und Hindernisse, NJW 2005, 2257.

[45] Wikipedia-Eintrag „E-Mail-Verschlüsselung", abrufbar unter https://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung.

[46] Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021, dort 1, Abs. 2; abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.

Bei personenbezogenen Daten, die nicht sensitiv sind, insbesondere nicht Besondere Kategorien von Daten nach Art. 9, 10 DSGVO darstellen, wird in der Regel eine Transportverschlüsselung bei Verarbeitung per E-Mail genügen, um ausreichenden Schutz zu gewährleisten. Dies setzt voraus, dass Sender und Empfänger ihre Mailsysteme entsprechend konfigurieren. Der Sender einer E-Mail muss sicherstellen, dass E-Mails nur dann versandt werden, wenn der Empfänger die entsprechende Verschlüsselung ebenfalls anwendet.[47]

4.2.1.2 Weitere, insbesondere organisatorische Maßnahmen

Neben den Fragen des Transports sind im Rahmen von technisch-organisatorischen Maßnahmen auch weitere Fragen zu behandeln. Dies betrifft etwa die Datensparsamkeit, indem etwa E-Mails nur an solche Personen weitergeleitet und verteilt werden, bei denen eine entsprechende Notwendigkeit der Kenntnisnahme besteht.

Zu regeln sind aber auch Fragen nach der Archivierung von E-Mails: diese liegen ja nun unverschlüsselt auf dem System des Empfängers (und meist wohl auch weiterhin denen des Senders) vor.

Besondere Bedeutung kommt zudem der Verwendung von E-Mail im Gesamt-Datenschutzkonzept von Unternehmen zu. Relevant sind hier etwa Richtlinien und Anweisungen, wie ein Informationszugang nach dem Need-to-know-Prinzip, IT-& Social Media-Guidelines, das Verbot der Privatnutzung von E-Mails, das Verbot der Datenspeicherung auf privaten Endgeräten oder das Senden betrieblicher Daten an private E-Mail-Adressen.[48]

Noch wenig beachtet sind zuletzt Fragen der Versendung von E-Mails als Datentransfer in Drittländer, mithin Länder, in denen weder die DSGVO gilt noch sonst ein angemessenes Datenschutzniveau sichergestellt ist.

4.2.2 E-Mails mit erhöhtem Schutzbedarf

In vielen Fällen werden beim Versand von E-Mails personenbezogene Daten mit erhöhtem Schutzbedarf verarbeitet. Die vorstehend diskutierten technisch-organisatorischen Maßnahmen reichen in diesem Fall nicht aus.

4.2.2.1 Besondere Kategorien von Daten (Art. 9, 10 DSGVO)

Artikel 9 und 10 DSGVO bestimmen Datenkategorien, die generell besonderen Schutz genießen. Hierzu gehören Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben sowie Daten über strafrechtliche Verurteilungen und Straftaten. Dies sind Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind. Sie verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten

[47] Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021, aaO., dort. 4.1.1. und 4.2.1.

[48] Vgl. für das Arbeitsverhältnis Fuhlrott/Fischer, Verschwiegenheitsklauseln im Lichte des Geschäftsgeheimnisschutzes, NZA 2022, 809, 811.

auftreten können.[49] Die Breite der aufgezählten Kategorien zeigt, dass jedenfalls im Sozialwesen, in der Medizin, in der Verwaltung, im Rechtswesen oder auch im Journalismus ständig solche besonderen Kategorien von Daten auch per E-Mail verarbeitet werden.

Bei solchen Daten, die unter Art. 9 oder 10 DSGVO fallen, sind in jedem Fall besondere Schutzmaßnahmen zu ergreifen, da insoweit schon aufgrund der allgemeinen datenschutzrechtlichen Wertung stets von einem hohen Risiko ausgegangen werden muss. Zumindest bei Unternehmen, die routinemäßig „sensible" Daten im Sinne von Art. 9 u. 10 DSGVO verarbeiten, ist es unvertretbar, dass die herkömmliche E-Mail noch Grundlage der Kommunikation ist.

4.2.2.2 Berufsgeheimnisträger

Bestimmte Personen, wie Rechtsanwältinnen und Rechtsanwälte sowie Ärztinnen und Ärzte, haben als Berufsgeheimnisträger besondere Pflichten zur Geheimhaltung ihnen anvertrauter Daten. Sie müssen neben dem Datenschutzrecht zusätzliche Strafvorschriften, z. B. § 203 StGB, und Berufsrecht beachten. Weil das Vorliegen eines Berufsgeheimnisses ein Indiz für ein hohes Risiko darstellen kann, haben Berufsgeheimnisträger die Höhe des jeweiligen Risikos besonders zu prüfen.

Auch wenn die DSGVO Berufsgeheimnisträger nicht ausdrücklich im Normtext adressiert, kann diese Eigenschaft in der Gesamtabwägung bezüglich des „angemessenen Schutzniveaus" eine Rolle spielen[50], aber muss für sich genommen noch nicht allein ausschlaggebend sein, um einen höheren Schutzbedarf zu begründen. Daher erscheint es sachgerecht, bei nicht von Art. 9 und 10 DSGVO erfassten Daten im Rahmen einer mandatsbezogenen Kommunikation von Rechtsanwälten als Berufsgeheimnisträger in Zweifelsfällen lediglich eine widerlegliche Vermutung[51] für einen besonderen Schutzbedarf der übermittelten Informationen zu sehen.[52] Diese widerlegbare Vermutung kann sich zur Gewissheit verdichten. Dies dürfte etwa im strafrechtlichen Bereich schon der Fall sein, wenn etwa ein „Interesse krimineller und ressourcenreicher Dritter" absehbar ist.[53]

Im Zweifel ist bei Kommunikation von Berufsgeheimnisträgern über E-Mail daher von erhöhtem Schutzbedarf auszugehen.

4.2.2.3 Erforderliche technisch-organisatorische Maßnahmen

Verantwortliche, die E-Mail-Nachrichten mit solch erhöhtem Schutzbedarf versenden[54], müssen regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen.[55]

---

[49] Erwägungsgrund 51 zur DSGVO.

[50] vgl. Erwägungsgrund. 75 S. 1 DSGVO: „Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten".

[51] Vgl. zur insoweit vergleichbaren Verschwiegenheitspflicht: Träger in Weyland, BRAO, 10. Aufl. 2020, § 43a Rn. 17.

[52] Vgl. VG Mainz, Urt. v. 17.12.2020 – 1 K 778/19.MZ, DStRE 2021, 1403, Rn. 34 ff.

[53] Vgl. Wagner BRAK-Mitteilungen 4/2019, 167, 172.

[54] Vgl. zur Frage, wann das der Fall ist, auch VG Mainz, Urt. v. 17.12.2020 – 1 K 778/19.MZ, rkr, DStRE 2021, 1403, Rn. 28 ff.

[55] Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021, aaO. dort 4.2.2.

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er sowohl eine qualifizierte Transportverschlüsselung als auch den Empfang von Ende-zu-Ende verschlüsselter Nachrichten ermöglichen.[56]

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei den der Bruch der Integrität ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er bestehende (PGP- oder S/MIME-) Signaturen qualifiziert prüfen.[57]

Bezüglich der sonstigen, insbesondere der organisatorischen Maßnahmen gelten, die oben diskutierten Grundsätze mit der Maßgabe, dass die Maßnahmen spezifisch an der Sensibilität der Daten auszurichten sind.

4.2.3 Gefahrgeneigtheit bezüglich weiterer Datenschutzverstöße

Determiniert durch den konzeptionellen Aufbau sind E-Mail-Programme gefahrgeneigt dergestalt, dass durch Unachtsamkeit oder Fehlbedienung leicht Datenschutzvorfälle entstehen. Das geschieht häufig etwa dadurch, dass Verteiler (und damit E-Mail-Adressen als personenbezogene Daten) offengelegt werden, weil sie im „Kopie"-Feld des Mail-Formulars verwendet werden. Ein bekanntes aktuelles Beispiel sind etwa 1500 Impftermine, die das Impfzentrum im Ennepe-Ruhr-Kreis absagte, und dabei die E-Mail-Adressen aller Impflinge sichtbar machte.[58]

4.3 Geheimnisschutz

Hinsichtlich des Schutzes von Geschäftsgeheimnissen gelten die obenstehend im Rahmen des Schutzes personenbezogener Daten diskutierten Gesichtspunkte entsprechend. Zwar liegt hier nicht notwendigerweise Personenbezug vor, die Fragen, die sich bezüglich Vertraulichkeit und Sicherheit stellen, sind jedoch weitgehend dieselben. Allerdings unterscheiden sich die Rechtsfolgen.

4.3.1 Verlust des Status als Geschäftsgeheimnis

Firmeninterne Geschäftsgeheimnisse können bei mangelhaftem Schutz ihren Status eben als Geschäftsgeheimnisse und damit ihre rechtliche Privilegierung verlieren, § 2 Nr. 1 b) des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG).

Geheimhaltungsmaßnahmen sind dabei alle Vorkehrungen, um die geheime Information vor einem rechtswidrigen Erlangen, Nutzen oder Offenlegen zu schützen. Erforderlich sind unternehmensspezifische

---

[56] Wie vor, Rn 4.1.2.

[57] Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021, 4.1.2; abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.

[58] Siehe Ruhr-Nachrichten vom 13.03.2021, „Datenschutz-Panne bei Impftermin-Absage im Ennepe-Ruhr-Kreis", Nachricht abrufbar unter https://www.ruhrnachrichten.de/regionales/datenschutz-panne-bei-impftermin-absage-im-ennepe-ruhr-kreis-w1614805-2000036498/.

Schutzkonzepte und Schutzstrategien, die ggf. an bestehende Sicherheitskonzepte aus anderen Bereichen anknüpfen können. Denkbar ist die Verbindung des Schutzes von Geschäftsgeheimnissen mit den zum Datenschutz erforderlichen Maßnahmen (vgl. Art. 28 Abs. 1 DSGVO: „geeignete technische und organisatorische Maßnahmen").[59] Hier kommen in technischer Hinsicht Maßnahmen in Betracht, die einen unbefugten Zugriff Dritter verhindern. Bei Daten wird dies bspw. regelmäßig die Zugangssicherung durch Passwörter, Verschlüsselungstechniken und dergleichen umfassen.[60] Salopp gesagt: was unter Datenschutzgesichtspunkten notwendig ist, wird auch im Geheimnisschutz geboten sein. Das gilt umso mehr für Betreiber kritischer Infrastruktur nach § 8a I BSI-Gesetz (*„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."*).

4.3.2 Verletzung von Geheimhaltungsvereinbarungen

Der Einsatz unverschlüsselter E-Mails bei der Übermittlung von vertraulichen Unterlagen oder Geschäftsgeheimnissen Dritter kann zudem einen Verstoß gegen Vertraulichkeitsvereinbarungen begründen. Ob und inwieweit dies der Fall ist, kann nur anhand der konkreten Geheimhaltungsvereinbarung beurteilt werden. Oft enthalten solche Vereinbarungen aber Klauseln dahingehend, dass für den Schutz der erfassten Geschäftsgeheimnisse mindestens die Sorgfalt anzuwenden ist, die auch für den Schutz eigener Geschäftsgeheimnisse des Verpflichteten notwendig und angemessen ist. Die betrifft aber gerade den vorgehend diskutierten Aspekt des GeschGehG: jedenfalls der Schutz, der durch dieses für den bloßen Erhalt des Status als Geschäftsgeheimnis gefordert wird, darf auch unter einer Geheimhaltungsvereinbarung erwartet werden.

4.4 E-Mail als Angriffsvektor und daraus resultierende Pflichten

Mehr als die Hälfte des weltweiten E-Mail-Aufkommens besteht aus sogenanntem Spam, also unerwünschten kommerziellen E-Mails.[61] Spam umfasst auch Phishing-Mails, mit denen Cyber-Kriminelle nach Passwörtern und anderen persönlichen Informationen fischen. Zuletzt dienen E-Mails als Werkzeug für die Übermittlung von Schadsoftware wie Viren, Würmern, Trojanern oder Ransomware.[62]

Neben der Gefahr für den eigenen Datenbestand besteht hierbei die Möglichkeit der Weiterverbreitung des Schadprogramms auf andere Nutzer. Selbst der private Nutzer ist daher verpflichtet, unbekannte und verdächtige Anhänge im Zweifelsfall ungeöffnet zu löschen bzw. nur nach Verifizierung des Absenders zu öffnen. Das Wissen um die Bedrohungen durch E-Mail-Anhänge darf heute zum allgemeinen Kenntnis-

[59] Vgl. Alexander, in Köhler/Bornkamm/Feddersen, UWG, 40. Auflage 2022, GeschGehG § 2 Rn. 53.

[60] Wie vor, Rn. 63.

[61] Laut Statista.de, abrufbar https://de.statista.com/statistik/daten/studie/872986/umfrage/anteil-der-spam-mails-am-gesamten-e-mail-verkehr-weltweit/.

[62] Teils ausgesprochen raffiniert, vgl. etwa Kaperung von E-Mail-Antwortketten: Was ist das und wie kann man sich schützen?, All About Security, abrufbar unter https://www.all-about-security.de/anwendungen-apps/kaperung-von-e-mail-antwortketten-was-ist-das-und-wie-kann-man-sich-schuetzen/.

stand des durchschnittlichen Internetnutzers gezählt werden. Besondere IT-Kenntnisse sind zur Durchführung der Maßnahme nicht erforderlich.[63] Dies muss erst recht für Unternehmen und Organisationen gelten.

Rechtsfolge der Verletzung entsprechender Sorgfaltspflichten können Schadensersatzansprüche unter dem Gesichtspunkt der Verletzung vertraglicher Nebenpflichten oder der deliktischen Haftung sein.

[63] Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, Rn. 311 f.

5 Ergebnis

Aufgrund ihrer technischen Eigenschaften, die aus Geschichte und Herkunft rühren, ist E-Mail kein per se sicheres Kommunikationsmedium. Dies gilt für nahezu alle Dimensionen (Beweiskraft, Datenschutz, Wahrung von Formvorschriften, Haftung für IT-Sicherheit, Geheimnisschutz etc.).

Im Rechtsverkehr bietet die herkömmliche E-Mail weder Gewissheit über die Authentizität des Absenders noch darüber, dass der Inhalt der Nachricht unverfälscht sein Ziel erreicht. Auch der Zugang einer E-Mail ist im Prozess nicht sicher beweisbar. Die herkömmliche E-Mail ist also als Kommunikationsmittel im Rechtsverkehr höchst riskant.

Datenschutzrechtlich ist die herkömmliche E-Mail aufgrund ihrer unzureichenden Verschlüsselung teilweise nicht ausreichend. Art. 32 Abs. 1 a) DSGVO nennt ausdrücklich die Verschlüsselung personenbezogener Daten als eine mögliche technische Maßnahme, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Daraus folgt, dass gerade bei sensiblen Daten (Art. 9 u. 10 DSGVO) oder Daten mit gesteigerter wirtschaftlicher Bedeutung und damit einer höheren Missbrauchsgefahr die herkömmliche E-Mail kein angemessenes Schutzniveau im Sinne von Art. 32 Abs. 1 DSGVO bietet.

Das gilt entsprechend auch für den Schutz von Geschäftsgeheimnissen. Ein mangelhafter Schutz - beispielsweise durch unverschlüsselte E-Mail - führt möglicherweise zum Verlust des rechtlichen Schutzes des Geheimnisses nach Maßgabe des GeschGehG.

Schließlich fördert das niedrige Sicherheitsniveau herkömmlicher E-Mails, nicht zuletzt auch durch Anwendungsfehler, das ständig steigende Aufkommen von Cyberkriminalität.

Wir kommen daher zum Ergebnis, dass die herkömmliche - nicht Ende-zu-Ende verschlüsselte - E-Mail zu einem erheblichen Teil des Geschäftsverkehrs nicht mehr den rechtlichen Anforderungen entspricht.

Kontaktdaten des Erstellers:
Dr. Maximilian Greger
Rechtsanwalt
Fachanwalt für IT-Recht
Fachanwalt für Urheber- und Medienrecht

Türkenstraße 16
80333 München

Tel.: +49 (0)89 28634-351